AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 635

109TH CONGRESS
2D SESSION

S. 3931

To establish procedures for the review of electronic surveillance programs.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 22, 2006

Mr. MCCONNELL (for himself and Mr. FRIST) introduced the following bill; which was read the first time pursuant to the order of September 21, 2006, as modified on September 22, 2006

SEPTEMBER 25, 2006

Read the second time and placed on the calendar

A BILL

To establish procedures for the review of electronic surveillance programs.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Terrorist Surveillance Act of 2006''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) After the terrorist attacks of September 11, 2001, President Bush authorized the National Security Agency to intercept communications between people inside the United States, including American citizens, and terrorism suspects overseas.

(2) One of the lessons learned from September 11, 2001, is that the enemies who seek to greatly harm and terrorize our Nation utilize technologies and techniques that defy conventional law enforcement practices.

(3) The President, as the constitutional officer most directly responsible for protecting the United States from attack, requires the ability and means to detect and track an enemy that can master and exploit modern technology.

(4) It is equally essential, however, that in protecting the United States against our enemies, the President does not compromise the very civil liberties that he seeks to safeguard. As Justice Hugo Black observed, ''The President's power, if any, to issue [an] order must stem either from an Act of Congress or from the Constitution itself.'' Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585 (1952) (opinion by Black, J.). Similarly, in 2004, Justice Sandra Day O'Connor explained in

her plurality opinion for the Supreme Court in Hamdi v. Rumsfeld: ''We have long since made clear that a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens.'' Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004) (citations omitted).

(5) When deciding issues of national security, it is in our Nation's best interest that, to the extent feasible, all 3 branches of the Federal Government should be involved. This helps guarantee that electronic surveillance programs do not infringe on the constitutional rights of Americans, while at the same time ensuring that the President has all the powers and means necessary to detect and track our enemies and protect our Nation from attack.

(6) As Justice Sandra Day O'Connor explained in her plurality opinion for the Supreme Court in Hamdi v. Rumsfeld, ''Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all 3 branches when individual liberties are at stake.'' Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004) (citations omitted).

(7) Similarly, Justice Jackson famously explained in his Youngstown concurrence: ''When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate ... When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility ... When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject.'' Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635–38 (1952) (Jackson, J., concurring).

(8) Congress clearly has the authority to enact legislation with respect to electronic surveillance programs. The Constitution provides Congress with broad powers of oversight over national security and foreign policy, under article I, section 8 of the Constitution of the United States, which confers on Congress numerous powers, including the powers—

(A) ''To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water'';

(B) ''To raise and support Armies'';

(C) ''To provide and maintain a Navy'';

(D) ''To make Rules for the Government and Regulation of the land and naval Forces'';

(E) ''To provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions''; and

(F) ''To provide for organizing, arming, and disciplining the Militia, and for governing such Part of them as may be employed in the Service of the United States''.

(9) While Attorney General Alberto Gonzales explained that the executive branch reviews the electronic surveillance program of the National Security Agency every 45 days to ensure that the program is

not overly broad, it is the belief of Congress that approval and supervision of electronic surveillance programs should be conducted outside of the executive branch, by the article III court established under section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803) and the congressional intelligence committees. It is also the belief of Congress that it is appropriate for an article III court to pass upon the constitutionality of electronic surveillance programs that may be directed at Americans.

(10) The Foreign Intelligence Surveillance Court is the proper court to approve and supervise classified electronic surveillance programs because it is adept at maintaining the secrecy with which it was charged and it possesses the requisite expertise and discretion for adjudicating sensitive issues of national security.

(11) In 1975, [then] Attorney General Edward Levi, a strong defender of executive authority, testified that in times of conflict, the President needs the power to conduct long-range electronic surveillance and that a foreign intelligence surveillance court should be empowered to issue special approval orders in these circumstances.

(12) Granting the Foreign Intelligence Surveillance Court the authority to review electronic surveillance programs and pass upon their constitutionality is consistent with well-established, longstanding practices.

(13) The Foreign Intelligence Surveillance Court already has broad authority to approve surveillance of members of international conspiracies, in addition to granting warrants for surveillance of a particular individual under sections 104, 105, and 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1804, 1805, and 1842).

(14) Prosecutors have significant flexibility in investigating domestic conspiracy cases. Courts have held that flexible warrants comply with the 4th amendment to the Constitution of the United States when they relate to complex, far-reaching, and multifaceted criminal enterprises like drug conspiracies and money laundering rings. The courts recognize that applications for search warrants must be judged in a common sense and realistic fashion, and the courts permit broad warrant language where, due to the nature and circumstances of the investigation and the criminal organization, more precise descriptions are not feasible.

(15) The Supreme Court, in the ''Keith Case'', United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297 (1972), recognized that the standards and procedures used to fight ordinary crime may not be applicable to cases involving national security. The Court recognized that national ''security surveillance may involve different policy and practical considerations from the surveillance of ordinary crime'' and that courts should be more flexible in issuing warrants in national security cases. United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 322 (1972).

(16) By authorizing the Foreign Intelligence Surveillance Court to review electronic surveillance programs, Congress enables the President to use the necessary means to guard our national security, while also protecting the civil liberties and constitutional rights that we cherish.

SEC. 3. DEFINITIONS.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended—

(1) by redesignating title VII as title VIII;

(2) by redesignating section 701 as section 801; and

(3) by inserting after title VI the following:

"TITLE VII—ELECTRONIC SURVEILLANCE PROGRAMS

"SEC. 701. DEFINITIONS.

''As used in this title—

''(1) the terms 'agent of a foreign power', 'Attorney General', 'contents', 'electronic surveillance', 'foreign power', 'international terrorism', 'minimization procedures', 'person', 'United States', and 'United States person' have the same meaning as in section 101;

''(2) the term 'congressional intelligence committees' means the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives;

''(3) the term 'electronic surveillance program' means a program to engage in electronic surveillance—

''(A) that has as a significant purpose the gathering of foreign intelligence information or protecting against international terrorism;

''(B) where it is not feasible to name every person, address, or location to be subjected to electronic surveillance;

''(C) where effective gathering of foreign intelligence information requires the flexibility to begin electronic surveillance immediately after learning of suspect activity; and

''(D) where effective gathering of foreign intelligence information requires an extended period of electronic surveillance;

''(4) the term 'foreign intelligence information' has the same meaning as in section 101(e) and includes information necessary to protect against international terrorism;

''(5) the term 'Foreign Intelligence Surveillance Court' means the court established under section 103(a); and

''(6) the term 'Foreign Intelligence Surveillance Court of Review' means the court established under section 103(b).''.

SEC. 4. FOREIGN INTELLIGENCE SURVEILLANCE COURT JURISDICTION TO REVIEW ELECTRONIC SURVEILLANCE PROGRAMS.

(a) IN GENERAL.—Title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 3, is amended by adding at the end the following:

"SEC. 702. FOREIGN INTELLIGENCE SURVEILLANCE COURT JURISDICTION TO REVIEW ELECTRONIC SURVEILLANCE PROGRAMS.

''(a) AUTHORIZATION OF REVIEW.—

''(1) INITIAL AUTHORIZATION.—The Foreign Intelligence Surveillance Court shall have jurisdiction to issue an order under this title, lasting not longer than 90 days, that authorizes an electronic surveillance program to obtain foreign intelligence information or to protect against international terrorism.

''(2) REAUTHORIZATION.—The Foreign Intelligence Surveillance Court shall have jurisdiction to reauthorize an electronic surveillance program for a period of time not longer than such court determines to be reasonable. There shall be no limit on the number of times the Attorney General may seek reauthorization of an electronic surveillance program.

''(3) RESUBMISSION OR APPEAL.—In the event that the Foreign Intelligence Surveillance Court refuses to approve an application under this subsection, the court shall state its reasons in a written opinion, which it shall submit to the Attorney General. The Attorney General or his designee may submit a new application under section 703 for the electronic surveillance program, with no limit on the

number of resubmissions that may be made. Alternatively, the Attorney General may appeal the decision of the Foreign Intelligence Surveillance Court to the Foreign Intelligence Surveillance Court of Review.

"(4) CONTINUED SURVEILLANCE UNDER TITLE I.—

"(A) IN GENERAL.—If, at any time, the Attorney General determines that the known facts and circumstances relating to any target within the United States under this title satisfy the criteria for an application under section 104 for an order for electronic surveillance of the target under section 105, the Attorney General shall—

"(i) discontinue the surveillance of the target under this title; or

"(ii) continue the surveillance of the target under this title, subject to the requirements of subparagraph (B).

"(B) CONTINUATION OF SURVEILLANCE.—

"(i) IN GENERAL.—The Attorney General may continue surveillance of a target under this title as specified in subparagraph (A)(ii) only if the Attorney General

makes an application under section 104 for an order for electronic surveillance of the target under section 105 as soon as the Attorney General determines practicable after the date on which the Attorney General makes the determination to continue surveillance of the target under subparagraph (A)(ii).

''(ii) PERIOD.—The period during which the Attorney General may continue surveillance of a target under this title after the Attorney General has determined that making an application is practicable shall be limited to a reasonable period, as determined by the Attorney General, during which the application is prepared and the period during which the application of the Attorney General under section 104 for an order for electronic surveillance of the target under section 105 is pending under title I, including during any period in which appeal from the denial of the application is pending with the Foreign Intelligence Surveillance Court of Review or the Supreme Court under section 103(b).

''(b) MANDATORY TRANSFER FOR REVIEW.—

''(1) IN GENERAL.—In any case before any court challenging the legality of classified communications intelligence activity relating to a foreign threat, including an electronic surveillance program, or in which the legality of any such activity or program is in issue, if the Attorney General files an affidavit under oath that the case should be transferred to the Foreign Intelligence Surveillance Court of Review because further proceedings in the originating court would harm the national security of the United States, the originating court shall transfer the case of the Foreign Intelligence Surveillance for further proceedings under this subsection.

''(2) PROCEDURES FOR REVIEW.—The Foreign Intelligence Surveillance Court shall have jurisdiction as appropriate to determine standing and the legality of the program to the extent necessary for resolution of the underlying case. All proceedings under this paragraph shall be conducted in accordance with the procedures set forth in section 106(f). In the event the Foreign Intelligence Surveillance Court determines that, in the context of a criminal proceeding, the Constitution of the United States would require the disclosure of national security in-

formation, any such constitutionally required disclosure shall be governed by the Classified Information Procedures Act, (18 U.S.C. App.), or if applicable, section 2339B(f) of title 18, United States Code.

''(3) APPEAL, CERTIORARI, AND EFFECTS OF DECISIONS.—The decision of the Foreign Intelligence Surveillance Court made under paragraphs (1) and (2), including a decision that the disclosure of national security information is constitutionally required, shall be subject to review by the Foreign Intelligence Surveillance Court of Review under section 103(b). The Supreme Court of the United States shall have jurisdiction to review decisions of the Foreign Intelligence Surveillance Court of Review by writ of certiorari granted upon the petition of the United States. The decision by the Foreign Intelligence Surveillance Court shall otherwise be binding in all other courts.

''(4) DISMISSAL.—The Foreign Intelligence Surveillance Court or a court that is an originating court under paragraph (1) may dismiss a challenge to the legality of an electronic surveillance program for any reason provided for under law.

''(5) PRESERVATION OF LITIGATION PRIVILEGES.—Nothing in this Act shall be construed to

abrogate, limit, or affect any litigation privileges in any court.''.

SEC. 5. APPLICATIONS FOR APPROVAL OF ELECTRONIC SURVEILLANCE PROGRAMS.

Title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 4, is amended by adding at the end the following:

''SEC. 703. APPLICATIONS FOR APPROVAL OF ELECTRONIC SURVEILLANCE PROGRAMS.

''(a) IN GENERAL.—Each application for approval of an electronic surveillance program under this title (including resubmission or application for reauthorization) shall—

''(1) be made by the Attorney General or his designee;

''(2) include a statement of the authority conferred on the Attorney General by the President of the United States;

''(3) include a statement setting forth the legal basis for the conclusion by the Attorney General that the electronic surveillance program is consistent with the Constitution of the United States;

''(4) certify that a significant purpose of the electronic surveillance program is to obtain foreign

intelligence information or to protect against international terrorism;

''(5) certify that the information sought cannot reasonably be obtained by normal investigative techniques

''(6) certify that the information sought cannot reasonably be obtained through an application under section 104;

''(7) include a statement of the means and operational procedures by which the electronic surveillance will be executed and effected;

''(8) include an explanation of how the electronic surveillance program is reasonably designed to ensure that the communications that are acquired are communications of or with—

''(A) a foreign power that engages in international terrorism or activities in preparation therefor;

''(B) an agent of a foreign power that engages in international terrorism or activities in preparation therefor;

''(C) a person reasonably believed to have communication with or be associated with a foreign power that engages in international terrorism or activities in preparation therefor or

an agent of a foreign power that engages in international terrorism or activities in preparation therefor; or

''(D) a foreign power that poses an imminent threat of attack likely to cause death, serious injury, or substantial economic damage to the United States, or an agent of a foreign power thereof;

''(9) include a statement of the proposed minimization procedures;

''(10) if the electronic surveillance program that is the subject of the application was initiated prior to the date the application was submitted, specify the date that the program was initiated;

''(11) include a description of all previous applications that have been made under this title involving the electronic surveillance program in the application (including the minimization procedures and the means and operational procedures proposed) and the decision on each previous application; and

''(12) include a statement of facts concerning the implementation of the electronic surveillance program described in the application, including, for any period of operation of the program authorized not

less than 90 days prior to the date of submission of the application—

''(A) the minimization procedures implemented; and

''(B) the means and operational procedures by which the electronic surveillance was executed and effected.

''(b) ADDITIONAL INFORMATION.—The Foreign Intelligence Surveillance Court may require the Attorney General to furnish such other information as may be necessary to make a determination under section 704.''.

SEC. 6. APPROVAL OF ELECTRONIC SURVEILLANCE PROGRAMS.

Title VII of the Foreign Intelligence Surveillance Act 18 of 1978, as amended by section 5, is amended by adding at the end the following:

''SEC. 704. APPROVAL OF ELECTRONIC SURVEILLANCE PROGRAMS.

''(a) NECESSARY FINDINGS.—Upon receipt of an application under section 703, the Foreign Intelligence Surveillance Court shall enter an ex parte order as requested, or as modified, approving the electronic surveillance program if it finds that—

''(1) the President has authorized the Attorney General to make the application for electronic sur-

veillance for foreign intelligence information or to protect against international terrorism;

''(2) approval of the electronic surveillance program in the application is consistent with the Constitution of the United States;

''(3) the electronic surveillance program is reasonably designed to ensure that the communications that are acquired are communications of or with—

''(A) a foreign power that engages in international terrorism or activities in preparation therefor;

''(B) an agent of a foreign power that is engaged in international terrorism or activities in preparation therefor;

''(C) a person reasonably believed to have communication with or be associated with a foreign power that is engaged in international terrorism or activities in preparation therefor or an agent of a foreign power that is engaged in international terrorism or activities in preparation therefor; or

''(D) a foreign power that poses an imminent threat of attack likely to cause death, serious injury, or substantial economic damage to

the United States, or an agent of a foreign power thereof;

''(4) the proposed minimization procedures meet the definition of minimization procedures under section 101(h); and

''(5) the application contains all statements and certifications required by section 703.

''(b) CONSIDERATIONS.—In considering the constitutionality of the electronic surveillance program under subsection (a), the Foreign Intelligence Surveillance Court may consider—

''(1) whether the electronic surveillance program has been implemented in accordance with the proposal by the Attorney General, by comparing—

''(A) the minimization procedures proposed with the minimization procedures actually implemented;

''(B) the nature of the information sought with the nature of the information actually obtained; and

''(C) the means and operational procedures proposed with the means and operational procedures actually implemented; and

''(2) whether foreign intelligence information has been obtained through the electronic surveillance program.

''(c) CONTENTS OF ORDER.—An order approving an electronic surveillance program under this section shall direct—

''(1) that the minimization procedures be followed;

''(2) that, upon the request of the applicant, specified communication or other common carriers, landlords, custodians, or other specified persons, furnish the applicant forthwith with all information, facilities, or technical assistance necessary to undertake the electronic surveillance program in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carriers, landlords, custodians, or other persons are providing potential targets of the electronic surveillance program;

''(3) that any records concerning the electronic surveillance program or the aid furnished or retained by such carriers, landlords, custodians, or other persons are maintained under security procedures approved by the Attorney General and the Director of National Intelligence; and

''(4) that the applicant compensate, at the prevailing rate, such carriers, landlords, custodians, or other persons for furnishing such aid.''.

SEC. 7. CONGRESSIONAL OVERSIGHT.

Title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 6, is amended by adding at the end the following:

''SEC. 705. CONGRESSIONAL OVERSIGHT.

''(a) IN GENERAL.—Not less often than every 180 days, the Attorney General shall submit to the congressional intelligence committees a report in classified form on the activities during the previous 180-day period under any electronic surveillance program authorized under this title.

''(b) CONTENTS.—Each report submitted under subsection (a) shall provide, with respect to the previous 180-day period, a description of—

''(1) the minimization procedures implemented;

''(2) the means and operational procedures by which the electronic surveillance program was executed and effected;

''(3) significant decisions of the Foreign Intelligence Surveillance Court on applications made under section 703;

''(4) the total number of applications made for orders approving electronic surveillance programs pursuant to this title; and

''(5) the total number of orders applied for that have been granted, modified, or denied.

''(c) RULE OF CONSTRUCTION.—Nothing in this title shall be construed to limit the authority or responsibility of any committee of either House of Congress to obtain such information as such committee may need to carry out its respective functions and duties.''.

SEC. 8. CLARIFICATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) REPEAL.—Sections 111, 309, and 404 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1811, 1829, and 1844) are repealed.

(b) CLARIFYING AMENDMENTS.—

(1) TITLE 18.—Section 2511(2) of title 18, United States Code, is amended—

(A) in paragraph (e), by striking '', as defined in section 101'' and all that follows through the end of the paragraph and inserting the following: ''under the Constitution or the Foreign Intelligence Surveillance Act of 1978.''; and

(B) in paragraph (f), by striking ''from international or foreign communications,'' and all that follows through the end of the paragraph and inserting ''that is authorized under a Federal statute or the Constitution of the United States.''.

(2) FISA.—Section 109 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1809) is amended—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by striking ''authorized by statute'' and inserting ''authorized by law''; and

(II) by striking ''or'' at the end;

(ii) in paragraph (2)—

(I) by striking ''authorized by statute'' and inserting ''authorized by law''; and

(II) by striking the period and inserting ''; or''; and

(iii) by adding at the end the following:

''(3) and knowingly discloses or uses information obtained under color of law by electronic sur-

veillance in a manner or for a purpose not authorized by law.''; and

(B) in subsection (c)—

(i) by striking ''$10,000'' and inserting ''$100,000''; and

(ii) by striking ''five years'' and inserting ''15 years''.

SEC. 9. MODERNIZING AMENDMENTS TO FISA.

(a) REFERENCE.—In this section, a reference to ''FISA'' shall mean the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) DEFINITIONS.—Section 101 of FISA (50 U.S.C. 1801) is amended—

(1) in subsection (b)(1)—

(A) in subparagraph (C), by striking ''or'' after the semicolon; and

(B) by adding at the end the following:

''(D) otherwise is reasonably expected to possess, control, transmit, or receive foreign intelligence information while that person is in the United States, provided that the official making the certification required by section 104(a)(6) deems such foreign intelligence information to be significant; or'';

(2) by striking subsection (f) and inserting the following:

''(f) 'Electronic surveillance' means—

''(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing the surveillance at a particular known person who is reasonably believed to be in the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or

''(2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are reasonably believed to be located within the United States.'';

(3) in subsection (h), by striking paragraph (4) and inserting the following:

''(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102 or 704, procedures that require that no contents of any communication originated or sent by a United States person shall

be disclosed, disseminated, used or retained for longer than 7 days unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.''.

(4) by striking subsection (l); and

(5) by striking subsection (n) and inserting the following:

''(n) 'contents', when used with respect to a communication, includes any information concerning the substance, symbols, sounds, words, purport, or meaning of a communication, and does not include dialing, routing, addressing, or signaling information.''.

(c) ELECTRONIC SURVEILLANCE AUTHORIZATION.—Section 102 of FISA (50 U.S.C. 1802) is amended to read as follows:

''ELECTRONIC SURVEILLANCE AUTHORIZATION WITHOUT COURT ORDER; CERTIFICATION BY ATTORNEY GENERAL; REPORTS TO CONGRESSIONAL COMMITTEES; TRANSMITTAL UNDER SEAL; DUTIES AND COMPENSATION OF COMMUNICATION COMMON CARRIER; APPLICATIONS; JURISDICTION OF COURT

''SEC. 102. (a)(1) Notwithstanding any other law, the President through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods

of up to 1 year if the Attorney General certifies in writing under oath that the electronic surveillance is directed at—

"(A)(i) the acquisition of the contents of communications of foreign powers, as defined in paragraph (1), (2), or (3) of section 101(a), or a person other than a United States person acting as an agent of a foreign power, as defined in section 101(b)(1)(A) or (B); or

"(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a); and

"(B) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h);

if the Attorney General reports such minimization procedures and any changes thereto to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives at least 30 days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

''(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures. The Attorney General shall assess compliance with such procedures and shall report such assessments to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives under section 108(a). If an electronic surveillance authorized by this subsection is directed at an agent of a foreign power, the Attorney General's report assessing compliance with the minimization procedures shall also include a statement of the facts and circumstances relied upon to justify the belief that the target of the electronic surveillance is an agent of a foreign power.

''(3) The Attorney General shall immediately transmit under seal to the court established under section 103(a) a copy of any certification under this subsection. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless—

''(A) an application for a court order with respect to the surveillance is made under section 104; or

''(B) the certification is necessary to determine the legality of the surveillance under section 106(f).

''(b)(1) Notwithstanding any other provision of law, the President, through the Attorney General, may authorize the acquisition of foreign intelligence information for periods of up to 1 year concerning a person reasonably believed to be outside the United States if the Attorney General certifies in writing under oath that he has determined that—

''(A) the acquisition does not constitute electronic surveillance as defined in section 101(f);

''(B) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a wire or electronic communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person thereof) who has access to wire or electronic communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;

''(C) a significant purpose of the acquisition is to obtain foreign intelligence information; and

''(D) the minimization procedures to be employed with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

''(2) Such certification need not identify the specific facilities, places, premises, or property at which the acquisition will be directed.

''(3) An acquisition undertaken pursuant to this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by the Attorney General. The Attorney General shall assess compliance with such procedures and shall report such assessments to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives under section 108(a).

''(4) The Attorney General shall immediately transmit under seal to the court established under section 103(a) a copy of any certification of the Attorney General under this subsection. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless the certification is nec-

essary to determine the legality of the acquisition under subsection (o).

''(c) With respect to the acquisition authorized under this section, the Attorney General may direct a specified person to—

''(1) furnish the government forthwith all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect its secrecy and produce a minimum of interference with the services that such person is providing to the target; and

''(2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such person wishes to maintain.

''(d) The government shall compensate, at the prevailing rate, such specified person for furnishing the aid set forth in subsection (c).

''(e) In the case of a failure to comply with a directive issued pursuant to this section, the Attorney General may invoke the aid of the court established under section 103(a) to compel compliance with the directive. The court shall issue an order requiring the person or entity to comply with the directive forthwith if it finds that the directive

was issued in accordance with subsection (a) or (b) and is otherwise lawful. Any failure to obey the order of the court may be punished by the court as contempt thereof. Any process under this section may be served in any judicial district in which the person or entity may be found.

''(f)(1)(A) A person receiving an Attorney General directive issued pursuant to this section may challenge the legality of that directive by filing a petition with the pool established by section 103(e)(1).

''(B) The presiding judge shall immediately assign a petition to one of the judges serving in the pool established by section 103(e)(1). Not later than 24 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the directive. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the directive or any part thereof that is the subject of the petition. If the assigned judge determines the petition is not frivolous, the assigned judge shall within 72 hours consider the petition in accordance with the procedures established under section 103(e)(2) and provide a written statement for the record of the reasons for any determination under this subsection.

''(2) A judge considering a petition to modify or set aside a directive may grant such petition only if the judge

finds that such directive does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the directive, the judge shall immediately affirm such directive, and order the recipient to comply therewith.

''(3) Any directive not explicitly modified or set aside consistent with this subsection shall remain in full effect.

''(g) A petition for review of a decision under subsection (f) to affirm, modify, or set aside a directive by the Government or any person receiving such directive shall be made within 7 days of issuance of the decision required by subsection (f) to the court of review established under section 103(b), which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such directive for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

''(h) Judicial proceedings under this section shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice

of the United States, in consultation with the Attorney General and the Director of National Intelligence.

''(i) All petitions under this section shall be filed under seal. In any proceedings under this section, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions thereof, which may include classified information.

''(j) No cause of action shall lie in any court against any provider of a communication service or other person (including any officer, employee, agent, or other specified person thereof) for furnishing any information, facilities, or assistance in accordance with a directive under subsection (a) or (b).

''(k) Information acquired pursuant to an Attorney General authorization under this section concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by subsection (a) or (b), as applicable. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this section shall lose its privileged character. No information from an acquisition under this section may be used or disclosed by Federal officers or employees except for lawful purposes.

''(l) No information acquired pursuant to this section shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

''(m) Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an acquisition under this section, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

''(n) Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information

obtained or derived from an acquisition under this section, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

''(o) Any person against whom evidence obtained or derived from an acquisition authorized pursuant to this section to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such acquisition on the grounds that—

''(1) the information was unlawfully acquired; or

''(2) the acquisition was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

''(p) Whenever a court or other authority is notified pursuant to subsection (m) or (n), whenever a motion is

made pursuant to subsection (o), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain an Attorney General directive or other materials relating to the acquisition authorized under this section or to discover, obtain, or suppress evidence or information obtained or derived from the acquisition authorized under this section, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the directive, and such other materials relating to the acquisition as may be necessary to determine whether the acquisition authorized under this section was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the directive or other materials relating to the acquisition only where such disclosure is necessary to make an accurate determination of the legality of the acquisition.

''(q) If the United States district court pursuant to subsection (o) determines that the acquisition authorized under this section was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived or otherwise grant the motion of the aggrieved person. If the court determines that such acquisition was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

''(r) Orders granting motions or requests under subsection (o), decisions under this section that an acquisition was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of directives or other materials relating to such acquisition shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

''(s) Federal officers who acquire foreign intelligence information under this section may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law

enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against—

''(1) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

''(2) sabotage, international terrorism, or the development or proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

''(3) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

''(t) Coordination authorized by subsection (s) shall not preclude the certification required by subsection (a) or (b), as applicable.

''(u) RETENTION OF DIRECTIVES AND ORDERS.—Directives made and orders granted under this section shall be retained for a period of at least 10 years from the date when they were made.''.

(d) DESIGNATION OF JUDGES.—Section 103 of FISA (50 U.S.C. 1803) is amended—

(1) in subsection (a), by inserting, ''at least'' before ''seven of the United States judicial circuits''; and

(2) at the end by adding the following new subsection:

''(g) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under this section, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information.''.

(e) APPLICATIONS FOR COURT ORDERS.—Section 104 of FISA (50 U.S.C. 1804) is amended—

(1) in subsection (a), by striking paragraphs (6) through (11) and inserting the following:

''(6) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official authorized by the President to conduct electronic surveillance for foreign intelligence purposes—

''(A) that the certifying official deems the information sought to be foreign intelligence information;

''(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

''(C) that such information cannot reasonably be obtained by normal investigative techniques; and

''(D) including a statement of the basis for the certification that—

''(i) the information sought is the type of foreign intelligence information designated; and

''(ii) such information cannot reasonably be obtained by normal investigative techniques;

''(7) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this title should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter;

''(8) a summary description of the nature of the information sought and the type of communications or activities to be subject to the surveillance;

''(9) a summary statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application; and

''(10) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance.'';

(2) by striking subsection (b);

(3) by redesignating subsections (c) through (e) as subsections (b) through (d), respectively; and

(4) in subsection (d)(1)(A), as redesignated by paragraph (3), by inserting after ''Secretary of State'' inserting ''Director of the Central Intelligence Agency''.

(f) ISSUANCE OF ORDER.—Section 105 of FISA (50 U.S.C. 1805) is amended—

(1) in subsection (a), by—

(A) striking paragraph (1); and

(B) redesignating paragraphs (2) through (5) as paragraphs (1) through (4), respectively;

(2) by striking paragraph (1) of subsection (c) and inserting the following:

''(1) An order approving an electronic surveillance under this section shall specify—

''(A) the identity, if known, or a description of the target of the electronic surveillance identified or described in the application pursuant to section 104(a)(3);

''(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;

''(C) the period of time during which the electronic surveillance is approved;

''(D) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance; and

''(E) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance.'';

(3) by striking subsection (d) and inserting the following:

''(d) Each order under this section shall specify the type of electronic surveillance involved, including whether physical entry is required.'';

(4) by striking paragraph (2) of subsection (e) and inserting the following:

''(2) Extensions of an order issued under this title may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order and may be for a period not longer than the court determines to be reasonable or 1 year, whichever is less.'';

(5) by striking subsection (f) and inserting the following:

''(f)(1) Notwithstanding any other provision of this title, when an executive branch officer appointed by the President with the advice and consent of the Senate who is authorized by the President to conduct electronic surveillance reasonably determines that—

''(A) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and

''(B) the factual basis for issuance of an order under this title to approve such surveillance exists;

that official may authorize the emergency employment of electronic surveillance in accordance with paragraph (2).

''(2) Under paragraph (1), the following requirements shall be satisfied:

''(A) The Attorney General shall be informed of the emergency electronic surveillance.

''(B) A judge having jurisdiction under section 103 shall be informed by the Attorney General or his designee as soon as practicable following such authorization that the decision has been made to employ emergency electronic surveillance.

''(C) An application in accordance with this title shall be made to that judge or another judge having jurisdiction under section 103 as soon as practicable, but not more than 7 days after such surveillance is authorized. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of emergency authorization, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information ob-

tained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 103.

''(D) The official authorizing the emergency employment of electronic surveillance shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.''; and

(6) in subsection (i)—

(A) by striking ''a wire or'' and inserting ''any'';

(B) by striking ''chapter'' and inserting ''title''; and

(C) by adding at the end '', or in response to certification by the Attorney General or his designee seeking information, facilities, or technical assistance from such person under section 102 of this title''.

(g) USE OF INFORMATION.—Section 106 of FISA (50 U.S.C. 1806) is amended—

(1) in subsection (i)—

(A) by striking ''radio''; and

(B) by inserting ''contain foreign intelligence information or'' after ''the Attorney General determines that the contents'' inserting ''contain foreign intelligence information or''; and

(2) in subsection (k), by striking ''1804(a)(7)'' and inserting ''104(a)(6)''.

(h) CONGRESSIONAL OVERSIGHT.—Section 108 of FISA (50 U.S.C. 1808) is amended by adding at the end the following:

''(c) DOCUMENT MANAGEMENT SYSTEM FOR APPLICATIONS FOR ORDERS APPROVING ELECTRONIC SURVEILLANCE.—

''(1) SYSTEM PROPOSED.—The Attorney General and Director of National Intelligence shall, in consultation with the Director of the Federal Bureau of Investigation, the Director of the National Security Agency, the Director of the Central Intelligence Agency, and the court established under section 103(b), conduct a feasibility study to develop and implement a secure, classified document management system that permits the prompt preparation, modification, and review by appropriate personnel of the Department of Justice, the Federal Bureau of Investigation, the National Security Agency, and other applicable elements of the United States Government of applications under section 104 before their submittal to that court.

''(2) SCOPE OF SYSTEM.—The document management system proposed in paragraph (1) shall—

''(A) permit and facilitate the prompt submittal of applications and all other matters, including electronic filings, to the court established under section 103(b) under section 104 or 105(g)(5); and

''(B) permit and facilitate the prompt transmittal of rulings of that court to personnel

submitting applications described in paragraph (1).''.

(i) AMENDMENTS TO FISA TITLE I RELATING TO WEAPONS OF MASS DESTRUCTION.—

(1) Section 101 of FISA, as amended by subsection (b) of this section, is further amended—

(A) in subsection (b)(1)—

(i) by striking ''or'' at the end of subparagraph (D);

(ii) by redesignating subparagraph (E) as subparagraph (F); and

(iii) by inserting after subparagraph (D) the following new subparagraph (E):

''(E) engages in the development or proliferation of weapons of mass destruction, or activities in preparation therefor; or;'';

(B) in subsection (b)(2)(C), by striking ''sabotage or international terrorism'' and inserting ''sabotage, international terrorism, or the development or proliferation of weapons of mass destruction''; and

(C) by inserting after subsection (k) the following new subsection (l):

''(l) 'Weapon of mass destruction' means—

''(1) any destructive device (as that term is defined in section 921 of title 18, United States Code) that is intended or has the capability, to cause death or serious bodily injury to a significant number of people;

''(2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors;

''(3) any weapon involving a biological agent, toxin, or vector (as those terms are defined in section 178 of title 18, United States Code); or

''(4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.''.

(2) Sections 101(e)(1)(B), 106(k)(1)(B), and 305(k)(1)(B) of FISA are each amended by striking ''sabotage or international terrorism'' and inserting ''sabotage, international terrorism, or the development or proliferation of weapons of mass destruction''.

(j) CONFORMING AMENDMENTS TO TITLES I AND III OF FISA TO ACCOMMODATE INTERNATIONAL MOVEMENTS OF TARGETS.—

(1) Section 105(e) of FISA is amended by adding at the end the following new paragraph:

''(4) An order issued under this section shall remain in force during the authorized period of surveillance notwithstanding the absence of the target from the United States, unless the Government files a motion to extinguish the order and the court grants the motion.''.

(2) Section 304(d) of FISA is amended by adding at the end the following new paragraph:

''(4) An order issued under this section shall remain in force during the authorized period of physical search notwithstanding the absence of the target from the United States, unless the Government files a motion to extinguish the order and the court grants the motion.''.

SEC. 10. CONFORMING AMENDMENT TO TABLE OF CONTENTS.

The table of contents for the Foreign Intelligence Surveillance Act of 1978 is amended—

(1) by striking the item relating to section 102 and inserting the following new item:

''Sec. 102. Electronic surveillance authorization without court order; certification by attorney general; reports to congressional committees; transmittal under seal; duties and compensation of communication common carrier; applications; jurisdiction of court.'';

(2) by striking the items relating to sections 111, 309, and 404; and

(3) by striking the items related to title VII and section 701 and inserting the following:

"TITLE VII—ELECTRONIC SURVEILLANCE PROGRAMS

"TITLE VIII—EFFECTIVE DATE

Calendar No. 635

109TH CONGRESS
2D SESSION

S. 3931

A BILL

To establish procedures for the review of electronic surveillance programs.

SEPTEMBER 25, 2006

Read the second time and placed on the calendar